AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1 – 46. (Canceled)

47. (Currently Amended) A tamper-resistant electronic circuit for implementation in a device, said tamper-resistant electronic circuit comprising:

~~means~~ a storage device for tamper-resistantly storing a secret not accessible over an external circuit interface;

a receiver for receiving external data that is external to the tamper-resistant electronic circuit;

~~means~~ a cryptographic processing engine for performing cryptographic processing at least partly in response to said stored secret and external data received external to the tamper-resistant electronic circuit to generate ~~an~~ a temporal instance of device-specific security data internally confined within said electronic circuit during usage of said device, wherein the generated temporal instance of device-specific security data depends on a value of said stored secret and a value of said external data and wherein the generated temporal instance of device-specific security data can only be generated as long as external data is available at the receiver; and

~~means for performing~~ electronic circuitry configured to perform a security-related operation in response to said internally-confined temporal instance of device-specific security data.

48. (Previously Presented) The electronic circuit according to claim 47, wherein said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication.

49. (Currently Amended) The electronic circuit according to claim 47, wherein said device is configured for producing digital content and said security-related operation is configured for marking said digital content based on said internally-confined temporal instance of device-specific security data.

50. (Previously Presented) The electronic circuit according to claim 49, wherein said operation is configured for generating a device-specific fingerprint embedded into said digital content.

51. (Currently Amended) The electronic circuit according to claim 47, wherein said ~~means for performing cryptographic processing~~ cryptographic processing engine is configured for generating said internally-confined temporal instance of device-specific security data provided that additional input data in the form of predetermined trigger data is applied over an external circuit interface during usage of said device, wherein said trigger data is defined during configuration of said device.

52. (Previously Presented) The electronic circuit according to claim 51, wherein said trigger data is defined based on configurational device-specific security data provided during configuration of the device, and said electronic circuit further comprises:

means for generating, based on said stored secret and said configurational device-specific security data, said trigger data as a cryptographic representation of said configurational device-specific security data during configuration of said device;

means for outputting said cryptographic representation over an external circuit interface during configuration; and

means for internally re-generating said device-specific security data during usage of said device provided that said additional input corresponds to said cryptographic representation.

53. (Previously Presented) The electronic circuit according to claim 52, further comprising means for internally generating, during configuration of said device, said configurational device-specific security data at least partly based on said stored secret.

54. (Previously Presented) The electronic circuit according to claim 53, wherein said means for internally generating said configurational device-specific security data comprises means for generating a private key at least partly based on said stored secret, and said trigger data is generated as a cryptographic representation of said private key during configuration of said device.

55. (Currently Amended) The electronic circuit according to claim 47, further comprising means for making, during configuration of said device, said internally-confined temporal instance of device-specific security data available over an external circuit interface provided that a predetermined device access code is entered into the electronic circuit.

56. (Previously Presented) The electronic circuit according to claim 47, further comprising means for disabling internal access to at least one of said stored secret and said device-specific

security data unless a predetermined device access code is entered into the electronic circuit.

57. (Previously Presented) The electronic circuit according to claim 55, further comprising:

means for authentication of a manufacturer of said device;

means for providing, during device manufacturing, said device access code to said device manufacturer in response to successful authentication.

58. (Currently Amended) The electronic circuit according to claim 47, wherein said ~~means for performing a security-related operation based on said confined device-specific security data~~ electronic circuitry comprises:

means for performing additional cryptographic processing based on said internally-confined device-specific security data and further external input data to generate further security data; and

means for performing said security-related operation in response to said further security data.

59. (Previously Presented) The electronic circuit according to claim 58, wherein said device-specific security data represents a private key, and said further external input data represents an encryption of said further device-specific security data by the corresponding public key.

60. (Previously Presented) The electronic circuit according to claim 59, wherein said further security data represents a symmetric content decryption key issued by a content provider, and said device-specific security data represents a private key of a device manufacturer.

61. (Currently Amended) The electronic circuit according to claim 47, wherein said ~~means for performing cryptographic processing to generate device-specific security data~~ cryptographic processing engine is configured for generating a symmetric cryptographic key in response to a seed applied over an external circuit interface.

62. (Currently Amended) The electronic circuit according to claim 47, wherein said ~~means for performing cryptographic processing to generate device-specific security data~~ cryptographic processing engine is configured for generating ~~a~~ an internally-confined private key at least partly based on said stored secret, and said ~~means for performing a security-related operation~~ electronic circuitry comprises means for performing asymmetric cryptography operations based on said internally confined private key.

63. (Previously Presented) The electronic circuit according to claim 62, further comprising means for generating a public key corresponding to said private key during configuration of said device, and means for outputting said public key over an external circuit interface.

64. (Previously Presented) The electronic circuit according to claim 62, further comprising:

means for performing shared key generation to generate a new shared key based on said generated private key and a public key of an intended communication partner; and

means for performing cryptographic processing based on said new shared key.

65. (Currently Amended) The electronic circuit according to claim 47, wherein said ~~means for cryptographic processing~~ cryptographic processing engine is ~~operable~~ configured for generating said internally-confined temporal instance of device-specific security data ~~20~~ as a chain of k bind keys $B_1, \ldots, B_k$ in response to corresponding bind identities $R_1, \ldots, R_k$ according to the following formula:

$$B_i = f(B_{i-1}, R_i) \qquad \text{for } i=1, \ldots, k,$$

where B_0 represents the stored secret, and f is a cryptographic one-way function.

66. (Currently Amended) A device implemented with a tamper-resistant electronic circuit, said electronic circuit comprising:

~~means~~ a storage unit for tamper-resistantly storing a secret not accessible over an external circuit interface;

a receiver for receiving external data that is external to the tamper-resistant electronic circuit;

~~means~~ a cryptographic processing engine for performing cryptographic processing at least partly in response to said stored secret and external data received external to the tamper-resistant electronic circuit to generate ~~an~~ a temporal instance of device-specific security data internally confined within said electronic circuit during usage of said device, wherein the generated temporal instance of device-specific security data depends on a value of said stored secret and a value of said external data and wherein the generated temporal instance of device-specific security data can only be generated as long as external data is available at the receiver; and

~~means for performing~~ electronic circuitry configured to perform a security-related operation in response to said internally ~~-~~confined temporal instance of device-specific security data.

67. (Previously Presented) The device according to claim 66, wherein said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication.

68. (Previously Presented) The device according to claim 66, wherein said device is configured for producing digital content and said security-related operation is configured for marking said digital content based on said device-specific security data.

69. (Currently Amended) The device according to claim 66, wherein said ~~means for performing cryptographic processing~~ cryptographic processing engine is configured for generating said internally-confined temporal instance of device-specific security data provided that additional input data in the form of predetermined trigger data is applied over an external circuit interface of the electronic circuit during usage of said device, wherein said trigger data is defined during configuration of said device.

70. (Currently Amended) A method for management of security data for a device, said method comprising the steps of:

storing, in a controlled environment during manufacturing of a tamper-resistant electronic circuit, a secret randomized number in said electronic circuit such that the secret number is not available outside of said electronic circuit;

implementing, during circuit manufacturing, functionality into said electronic circuit for performing cryptographic processing at least partly based on said stored secret number and external data received external to the tamper-resistant electronic circuit to generate a temporal instance of device-specific security data internally confined within said electronic circuit during usage of the device, wherein the generated temporal instance of device-specific security data depends on a value of said stored secret and a value of said external data and

wherein the generated temporal instance of device-specific security data can only be generated as long as external data is available at the receiver;

implementing, during circuit manufacturing, a security-related operation into said electronic circuit, said security-related operation being configured for receiving at least said internally-confined temporal instance of device-specific security data as input during usage of the device; and

installing, during device manufacturing, said electronic circuit into said device.

71. (Previously Presented) The method according to claim 70, wherein said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication.

72. (Currently Amended) The method according to claim 70, wherein said device is configured for producing digital content and said security-related operation is configured for marking said digital content based on said internally-confined temporal instance of device-specific security data.

73. (Currently Amended) The method according to claim 70, further comprising the step of providing, during configuration of the device, trigger data to be applied later during usage of the device in order to be able to generate said internally-confined temporal instance of device-specific security data within said electronic circuit.

74. (Currently Amended) The method according to claim 73, further comprising the steps of:

entering, in a controlled environment during device configuration, said trigger data as input data into said electronic circuit in order to obtain device-specific security data from the cryptographic functionality of the electronic circuit;

recording, in a controlled environment during device configuration, said device-specific security data and said input data; and

entering, in a controlled environment during device configuration, a predetermined device access code into the electronic circuit for accessing the internally-confined temporal instance of device-specific security data over an external circuit interface.

75. (Currently Amended) The method according to claim 73, further comprising the steps of:

generating, in a controlled environment during device configuration, an internally-confined temporal instance of device-specific security data;

entering, in a controlled environment during device configuration, said generated device-specific security data into said electronic circuit in order to obtain said trigger data as a result representation from the cryptographic functionality of the electronic circuit; and

recording, in a controlled environment during device configuration, said result representation and the previously generated device-specific security data.